ACTA ARITHMETICA
LXXVI.4 (1996)

Fermat quotient of cyclotomic units

by

Tsutomu Shimada (Yokohama)

Introduction. Let p be an odd prime number, K a finite extension of the field of rational numbers $\mathbb{Q}$, O_K the ring of integers of K, and E_K its group of units. Let $\mathbb{N}$ be the set of natural numbers, and $\mathbb{Z}$ and $\mathbb{Z}_p$ be the ring of rational integers and the ring of p-adic integers, respectively.

We define

$$E_K(p^n) = \{u \in E_K : u \equiv 1 \bmod p^n\}, \qquad n \in \mathbb{N}.$$

For each $u \in E_K(p)$, we call

$$\frac{u-1}{p} \bmod p \quad (\in O_K/(p))$$

the *Fermat quotient* $\bmod p$ of u. That is, for a unit $u = 1 + px_u$, $x_u \in O_K$, $x_u \bmod p$ is the Fermat quotient $\bmod p$ of u. From now on, we omit "$\bmod p$" for simplicity.

We define a homomorphism $\psi\colon E_K(p) \to O_K/(p)$ by $u = 1 + px_u \mapsto x_u \bmod p$. Let $\mathbb{F}(K)$ denote the set of all Fermat quotients of $u \in E_K(p)$ or the image of ψ. Clearly, $\mathbb{F}(K)$ forms a subspace of $\mathbb{F}_p$-vector space $O_K/(p)$ where $\mathbb{F}_p$ denotes the field with p elements, and kernel of ψ is $E_K(p^2)$. So, we have

$$\mathbb{F}(K) \cong E_K(p)/E_K(p^2)$$

as $\mathbb{F}_p$-*vector spaces*.

Now, the following two statements are well known: first, if $\psi(u_1), \dots, \psi(u_s)$ are linearly independent over $\mathbb{F}_p$ then $u_1, \dots, u_s \in F_K(p)$ are $\mathbb{Z}_p$-independent, and secondly, the dimension of $E_K(p^n)/E_K(p^{n+1})$ over $\mathbb{F}_p$ equals the $\mathbb{Z}_p$-rank of $E_K(p)$ for sufficiently large n (see, Levesque [3] and Sands [4]). On the other hand, the Leopoldt conjecture states that $\mathbb{Z}_p$-rank of $E_K(p)$ equals $\mathbb{Z}$-rank of E_K.

The aim of the present article is to study the dimension of $\mathbb{F}(K)$ over $\mathbb{F}_p$, when K is a cyclotomic field.

1. Notations and results. Let $\zeta_n = \exp(2\pi i/n)$ for $n \in \mathbb{N}$, and let $m \in \mathbb{N}$ be odd, square free, $3 \leq m$ and prime to p. We let $K = \mathbb{Q}(\zeta_{mp})$ and let $E_K(p^n)$, $\mathbb{F}(K)$ and ψ be as in the introduction.

Since $O_K = \mathbb{Z}[\zeta_{mp}] = \mathbb{Z}[\zeta_m][1-\zeta_p]$ and m is square free, the set

$$\{\zeta_m^r(1-\zeta_p)^\nu : 1 \leq r \leq m,\ (r,m) = 1,\ \nu = 0,1,\dots,p-2\}$$

forms a $\mathbb{Z}$-basis of O_K. As is well known,

$$\dim_{\mathbb{F}_p}(\mathbb{Z}[\zeta_{mp}]/(p)) = [\mathbb{Q}(\zeta_{mp}) : \mathbb{Q}] = \varphi(mp),$$

where φ denotes the Euler function. Therefore, the set

$$\{\zeta_m^r(1-\zeta_p)^\nu \bmod p : 1 \leq r \leq m,\ (r,m) = 1,\ \nu = 0,1,\dots,p-2\}$$

forms an $\mathbb{F}_p$-basis of $O_K/(p)$.

Representing each $x \bmod p \in O_K/(p)$ in this basis, we have

$$x \equiv c_0 + c_1(1-\zeta_p) + c_2(1-\zeta_p)^2 + \dots + c_{p-2}(1-\zeta_p)^{p-2} \bmod p$$

with $c_i \in \mathbb{Z}[\zeta_m]$ $(i = 0,1,\dots,p-2)$, determined uniquely modulo p.

Let π denote $1-\zeta_p$ and let

$$E_K(p\pi^i) = \{u \in E_K : u \equiv 1 \bmod p\pi^i\} \qquad (i = 1,\dots,p-2).$$

Since

$$E_K(p) \supset E_K(p\pi) \supset \dots \supset E_K(p\pi^{p-2}) \supset E_K(p^2),$$

and $u^p \in E_K(p^2)$ for all $u \in E_K(p)$, we have

$$\mathbb{F}(K) = (E_K(p)/E_K(p\pi)) \oplus \dots \oplus (E_K(p\pi^{k+1})/E_K(p\pi^{k+2})) \oplus \dots \\ \dots \oplus (E_K(p\pi^{p-2})/E_K(p^2)).$$

Thus

$$\dim_{\mathbb{F}_p}\mathbb{F}(K) = \dim_{\mathbb{F}_p}(E_K(p)/E_K(p\pi)) + \dots \\ \dots + \dim_{\mathbb{F}_p}(E_K(p\pi^{k+1})/E_K(p\pi^{k+2})) + \dots \\ \dots + \dim_{\mathbb{F}_p}(E_K(p\pi^{p-2})/E_K(p^2)), \qquad -1 \leq k \leq p-3.$$

We define subsets V_k $(k = -1,0,1,\dots,p-3)$ of $\mathbb{F}(K)$ by

$$V_k = \{x_u \bmod p \in \mathbb{F}(K) : u \in E_K(p), \\ c_0 \equiv c_1 \equiv \dots \equiv c_k \equiv 0 \bmod p,\ c_{k+1} \not\equiv 0 \bmod p\},$$

where $u = 1 + px_u$ and $x_u \equiv c_0 + c_1(1-\zeta_p) + \dots + c_{p-2}(1-\zeta_p)^{p-2} \bmod p$, and $\widetilde{V}_k$ be the subspace generated by all elements in V_k over $\mathbb{F}_p$. Of course,

$$\mathbb{F}(K) = V_{-1} \cup V_0 \cup V_1 \cup \dots \cup V_{p-3} \cup \{0 \bmod p\} \qquad \text{(disjoint union)}.$$

For each k $(-1 \leq k \leq p-3)$, we define a mapping $\pi_k : \widetilde{V}_k \to \mathbb{Z}[\zeta_m]/(p)$ by $x_u \bmod p \mapsto c_{k+1} \bmod p$ and let $\overline{V}_k = \pi_k(\widetilde{V}_k)$. Then, since $\overline{V}_k \cong$

$E_K(p\pi^{k+1})/E_K(p\pi^{k+2})$ for $-1 \le k \le p-3$, we have

$$\dim_{\mathbb{F}_p} \mathbb{F}(K) = \sum_{k=-1}^{p-3} \dim_{\mathbb{F}_p} \overline{V}_k.$$

We now take polynomials $S_t(X) \in \mathbb{Q}[X]$, $\mathbb{Z} \ni t \ge 0$, such that $S_t(n) = 1^t + 2^t + \ldots + n^t$ for all $n \in \mathbb{N}$. For example,

$$S_0(X) = X, \quad S_1(X) = \tfrac{1}{2}X(X+1), \quad S_2(X) = \tfrac{1}{6}X(X+1)(2X+1), \quad \text{etc.}$$

As is well known, $(k+1)!S_k(X) \in \mathbb{Z}[X]$, $\deg S_k(X) = k+1$, and $S_k(-1) = 0$ for $k \ge 1$.

We define

$$I_k(n) = \sum_{l=1}^{n}{}' S_k\Big(-\frac{l}{n}\Big)\zeta_n^l, \qquad 0 \le k \le p-2,\ n \in \mathbb{N},$$

where $\sum_{l=1}^{n'}$ denotes the sum taken over all $l = 1, \ldots, n$ that are prime to n. Let G be the Galois group of $\mathbb{Q}(\zeta_m)$ over $\mathbb{Q}$ and $\widehat{G}$ its character group. As is well known, G is isomorphic to $(\mathbb{Z}/m\mathbb{Z})^\times$ (the multiplicative group of all residue classes prime to m) by assigning $\sigma_\mu : \zeta_m \mapsto \zeta_m^\mu$ to $\mu \bmod m$.

Note that ψ is a $\mathrm{Gal}(K/\mathbb{Q})$-homomorphism. We now state our results, Theorems 1–4.

THEOREM 1. (1) *There exist units $\alpha_k \in E_K(p)$, $1 \le k \le p-3$, such that*

$$\pi_k(\psi(\alpha_k)) = I_k(m) \bmod p.$$

(2) *For $k = 0$, there exists $\alpha_0 \in E_K(p)$ such that*

$$\pi_0(\psi(\alpha_0)) = (1-\sigma_p)I_0(m) \bmod p.$$

(3) *For $k = -1$, there exist $\beta_\nu \in E_K(p)$, $2 \le \nu \le m/2$ and $(\nu, m) = 1$, such that*

$$\pi_{-1}(\psi(\beta_\nu)) = (1-\sigma_\nu)I_{p-2}(m) \bmod p.$$

(4) *If $B_{k+1} \not\equiv 0 \bmod p$ for some $k = 1, 3, \ldots, p-4$, then there exists $u_k \in E_K(p)$ such that*

$$\pi_k(\psi(u_k)) = 1 \bmod p,$$

where B_n denote the Bernoulli numbers (the definition will be given in Section 4).

For any $a \in \mathbb{Z}$, let $M(a) \in \mathbb{Z}$ denote the non-negative minimal residue of $a \bmod m$, that is, $a \equiv M(a) \bmod m$ and $0 \le M(a) \le m-1$. When $b \in \mathbb{Z}$ is prime to m, we let $M(1/b) \in \mathbb{Z}$ be the integer such that $b \times M(1/b) \equiv 1 \bmod m$ and $0 \le M(1/b) \le m-1$. Also, we take $M(a/b)$ for $M(M(a) \times M(1/b))$.

For any $\sigma_r \in G$ and k $(0 \le k \le p-2)$,

$$I_k(m)^{\sigma_r} = \sum_{l=1}^{m}{}' S_k\Big(-\frac{l}{m}\Big)\zeta_m^{lr} = \sum_{l=1}^{m}{}' S_k\Big(-\frac{M(l/r)}{m}\Big)\zeta_m^{l}.$$

We then define for each k, $0 \le k \le p-2$, the matrix

$$\mathbf{A}_k(m) = \Big(S_k\Big(-\frac{M(l/r)}{m}\Big)\Big)_{\substack{1\le r,l\le m\\(r,m)=(l,m)=1}},$$

where we index the rows by r, and the columns by l. Since $I_k(m)^{\sigma_{-1}} = (-1)^{k+1}I_k(m)$ for $1 \le k \le p-2$ (see Lemma 3.2), we have $\operatorname{rank}\mathbf{A}_k(m) \le \frac{1}{2}\varphi(m)$ for such k.

In addition, we define

$$\mathbf{B}_k(m) = \Big(S_k\Big(-\frac{M(l/r)}{m}\Big)\Big)_{\substack{1\le r,l\le m/2\\(r,m)=(l,m)=1}}, \qquad 0 \le k \le p-2.$$

THEOREM 2. *For each k $(1 \le k \le p-3)$, we have*

$$\det\mathbf{B}_k(m) = \Big(\frac{-1}{2m^k}\Big)^{\varphi(m)/2}\zeta_{\mathbb{Q}(\zeta_m)^+}(-k)\prod_{\substack{\chi\in\widehat{G}\\ id.\neq\chi:even}}\prod_{q\mid m}(1-\chi_1(q)q^k) \times\Big(\prod_{q\mid m}(1-q^k)-m^k\varphi(m)\Big),$$

if k is odd, and

$$\det\mathbf{B}_k(m) = \Big(\frac{1}{2m^k}\Big)^{\varphi(m)/2}\frac{\zeta_{\mathbb{Q}(\zeta_m)}}{\zeta_{\mathbb{Q}(\zeta_m)^+}}(-k)\prod_{\widehat{G}\ni\chi:odd}\prod_{q\mid m}(1-\chi_1(q)q^k),$$

if k is even. Moreover, if $\det\mathbf{B}_k(m) \not\equiv 0 \bmod p$, then

$$\dim_{\mathbb{F}_p}\overline{V}_k \ge \tfrac{1}{2}\varphi(m).$$

Here $\zeta_{\mathbb{Q}(\zeta_m)}$ and $\zeta_{\mathbb{Q}(\zeta_m)^+}$ denote the Dedekind zeta functions of $\mathbb{Q}(\zeta_m)$ and $\mathbb{Q}(\zeta_m)^+$ (the maximal real subfield of $\mathbb{Q}(\zeta_m)$), respectively, and χ_1 the primitive Dirichlet character associated with χ. Also, $\prod_{q\mid m}$ denotes the product taken over all distinct primes q which divide m.

$\mathbf{B}_k(m)$ is, in some sense, a generalization of matrices defined by Carlitz [1] and Tateyama [5].

Let f be the order of the element $p \bmod m$ in $(\mathbb{Z}/m\mathbb{Z})^\times$, and $g = \varphi(m)/f$. Let $g(m)$ and $g^+(m)$ denote the number of distinct prime ideals which divide m in $\mathbb{Q}(\zeta_m)$ and $\mathbb{Q}(\zeta_m)^+$, respectively. We write $h^-(\mathbb{Q}(\zeta_m))$ for the relative class number of $\mathbb{Q}(\zeta_m)$. By the theorem of Tateyama [5], we can prove

THEOREM 3. *Assume $g(m) = g^+(m)$ and p does not divide $h^-(\mathbb{Q}(\zeta_m))$. Then*

$$\dim_{\mathbb{F}_p} \overline{V}_0 \geq \begin{cases} \frac{1}{2}\varphi(m) & \text{if } p \text{ does not decompose in } \mathbb{Q}(\zeta_m)/\mathbb{Q}(\zeta_m)^+, \\ \frac{1}{2}(\varphi(m) - g) & \text{if } p \text{ decomposes in } \mathbb{Q}(\zeta_m)/\mathbb{Q}(\zeta_m)^+. \end{cases}$$

Note that when the right-hand side in the inequality above is not positive, or $p \equiv 1 \bmod m$, our theorem says nothing. Finally, by the same calculation as in the proof of Theorem 2 we obtain:

THEOREM 4. *We have*

$$\det \mathbf{B}_{p-2}(m) = \left(\frac{-1}{2m^{p-2}}\right)^{\varphi(m)/2} \zeta_{\mathbb{Q}(\zeta_m)^+}(2-p) \prod_{\substack{\chi \in \widehat{G} \\ id. \neq \chi : even}} \prod_{q \mid m} (1 - \chi_1(q) q^{p-2}) \times \Big(\prod_{q \mid m} (1 - q^{p-2}) - m^{p-2}\varphi(m) \Big)$$

and if $\det \mathbf{B}_{p-2}(m) \not\equiv 0 \bmod p$, *then*

$$\dim_{\mathbb{F}_p} \overline{V}_{-1} \geq \tfrac{1}{2}\varphi(m) - 1.$$

The rest of the article will be devoted to the proofs of the theorems stated above. In Section 2, we discuss some elementary properties of the Fermat quotient of cyclotomic units. The main result here is Lemma 2.5. In Section 3, introducing $I_k(m)$, we prove Theorem 1(1). In Section 4, we prove Theorem 2 and the first part of Theorem 4. In Section 5, discussing $I_0(m)$ and the rank of $\mathbf{A}_0(m)$, we prove Theorem 1(2) and Theorem 3. In Section 6, by the argument in $\mathbb{Q}(\zeta_m)$, we prove Theorem 1(3) and the second part of Theorem 4. Finally, the proof of Theorem 1(4), which is obtained essentially in Washington [6], will be given in Section 7.

Before concluding this section, we classify typical generators of cyclotomic units (in the sense of Sinnot) into three types:

I. $1 - \zeta_d \zeta_p$ $\quad (1 \neq d \mid m)$,

II. $1 - \zeta_d$ $\quad (1 \neq d \mid m,\ d \text{ is composite})$,

$\dfrac{1 - \zeta_q^\nu}{1 - \zeta_q}$ $\quad (q \mid m,\ q \text{ is a prime}, 2 \leq \nu \leq q-1)$,

III. $\dfrac{1 - \zeta_p^\nu}{1 - \zeta_p}$ $\quad (2 \leq \nu \leq p-1)$.

We shall use cyclotomic units of type I to prove Theorem 1(1), (2), type II (units in $\mathbb{Q}(\zeta_m)$) to prove Theorem 1(3), and type III (units in $\mathbb{Q}(\zeta_p)$) to prove Theorem 1(4).

Also, see Leopoldt [2] for units of type II.

2. Fermat quotient of units of type I. We first prove a preliminary lemma:

LEMMA 2.1. *For each $\nu \in \mathbb{N}$, we have*

$$(1-X)^{p^\nu} \equiv 1 - X^{p^\nu} - p\left(X^{p^{\nu-1}} + \frac{X^{2p^{\nu-1}}}{2} + \ldots + \frac{X^{(p-1)p^{\nu-1}}}{p-1}\right) \bmod p^2.$$

P r o o f. We have

$$(1-X)^{p^\nu} = 1 - X^{p^\nu} + \sum_{i=1}^{p^\nu-1} \binom{p^\nu}{i} (-X)^i.$$

Since

$$\frac{(p^\nu-1)\ldots(p^\nu-i+1)}{(i-1)!} \equiv (-1)^{i-1} \bmod p^\nu,$$

we have

$$\binom{p^\nu}{i} \equiv \frac{(-1)^{i-1}}{i} p^\nu \bmod p^{2\nu-\mathrm{ord}_p i} \quad \text{for all } i = 1, \ldots, p^\nu - 1,$$

where $\mathrm{ord}_p i$ denotes the exact exponent of the power of p dividing i. Now, we have $2\nu - \mathrm{ord}_p i \geq 2\nu - (\nu-1) \geq 2$ and $\mathrm{ord}_p(p^\nu/i) \geq \nu - (\nu-1) = 1$. So, $\binom{p^\nu}{i} \not\equiv 0 \bmod p^2$ if and only if $\mathrm{ord}_p i = \nu - 1$, i.e. $i = jp^{\nu-1}$ for some j $(1 \leq j \leq p-1)$. If $i = jp^{\nu-1}$ $(1 \leq j \leq p-1)$, then

$$\binom{p^\nu}{i}(-X)^i \equiv \frac{(-1)^{i-1}}{j} p(-X)^i = -\frac{p}{j} X^{jp^{\nu-1}} \bmod p^2.$$

This completes the proof.

We define

$$f(X) = \frac{1}{1-X^p}\left(X + \frac{X^2}{2} + \ldots + \frac{X^{p-1}}{p-1}\right) \in \mathbb{Q}(X).$$

Using Lemma 2.1, we have

$$\begin{aligned}
(1-\zeta_m\zeta_p)^{p^{f+1}} &\equiv 1 - \zeta_m^{p^{f+1}} - p\left(\zeta_m^{p^f} + \frac{\zeta_m^{2p^f}}{2} + \ldots + \frac{\zeta_m^{(p-1)p^f}}{p-1}\right) \\
&= 1 - \zeta_m^p - p\left(\zeta_m + \frac{\zeta_m^2}{2} + \ldots + \frac{\zeta_m^{p-1}}{p-1}\right) \\
&= (1-\zeta_m^p)(1 - pf(\zeta_m)) \bmod p^2, \\
(1-\zeta_m\zeta_p)^p &\equiv 1 - \zeta_m^p - p\left(\zeta_m\zeta_p + \frac{\zeta_m^2\zeta_p^2}{2} + \ldots + \frac{\zeta_m^{p-1}\zeta_p^{p-1}}{p-1}\right) \\
&= (1-\zeta_m^p)(1 - pf(\zeta_m\zeta_p)) \bmod p^2,
\end{aligned}$$

and so

$$(1-\zeta_m\zeta_p)^{p^{f+1}-p} \equiv 1 - p(f(\zeta_m) - f(\zeta_m\zeta_p)) \bmod p^2.$$

Consequently, $f(\zeta_m)-f(\zeta_m\zeta_p) \bmod p$ belongs to $\mathbb{F}(K)$. Note that $(O_K/(p))^\times$ (the multiplicative group of $O_K/(p)$) has the exponent $p^{f+1}-p$. We first prove the existence of a "canonical" element in $\mathbb{F}(K)$, a linear combination over $\mathbb{F}_p$ of conjugates of $f(\zeta_m) - f(\zeta_m\zeta_p) \bmod p$ (see Lemma 2.3), and next determine the coefficients $\bmod p$ of its image by π_k (see Lemma 2.5). From $\zeta_p^j = ((\zeta_p - 1) + 1)^j$, it can be easily seen that

$$1 - \zeta_p^j = \sum_{i=1}^{j} \binom{j}{i} (-1)^{i+1} (1-\zeta_p)^i.$$

Hence

$$\begin{aligned}(1)\qquad f(\zeta_m) - f(\zeta_m\zeta_p) &= \frac{1}{1-\zeta_m^p} \sum_{j=1}^{p-1} \frac{\zeta_m^j}{j}(1-\zeta_p^j) \\ &= \frac{1}{1-\zeta_m^p} \sum_{j=1}^{p-1} \sum_{i=1}^{j} \frac{\zeta_m^j}{j} \binom{j}{i} (-1)^{i+1}(1-\zeta_p)^i \\ &= \frac{1}{1-\zeta_m^p} \sum_{i=1}^{p-1} \sum_{j=i}^{p-1} \frac{\zeta_m^j}{j} \binom{j}{i} (-1)^{i+1}(1-\zeta_p)^i,\end{aligned}$$

that is,

$$f(\zeta_m) - f(\zeta_m\zeta_p) = \frac{1}{1-\zeta_m^p} \sum_{i=1}^{p-1} \left(\sum_{j=1}^{p-1} \frac{\binom{j}{i}}{j} \zeta_m^j \right) (-1)^{i+1}(1-\zeta_p)^i,$$

where $\binom{j}{i} = 0$ if $j < i$.

LEMMA 2.2. *For each $\nu = 1, \dots, p-1$ we have*

$$f(\zeta_m) - f(\zeta_m\zeta_p^\nu) \equiv \frac{1}{1-\zeta_m^p} \sum_{i=1}^{p-2} \left(\sum_{j=1}^{p-1} \frac{\binom{\nu j}{i}}{j} \zeta_m^j \right) (-1)^{i+1}(1-\zeta_p)^i \bmod p.$$

Proof. Taking ζ_p^ν for ζ_p in both sides of (1), we get

$$f(\zeta_m) - f(\zeta_m\zeta_p^\nu) = \frac{1}{1-\zeta_m^p} \sum_{j=1}^{p-1} \frac{\zeta_m^j}{j}(1-\zeta_p^{\nu j}).$$

We denote by $P(a)$ $(a \in \mathbb{Z})$ the non-negative minimal residue of $a \bmod p$ and use it similarly to $M(a)$ introduced in the previous section. Then

$$\sum_{j=1}^{p-1}\frac{\zeta_m^j}{j}(1-\zeta_p^{\nu j})$$

$$\equiv \sum_{j=1}^{p-1}\frac{\zeta_m^{P(j/\nu)}}{j/\nu}(1-\zeta_p^j)$$

$$= \nu\sum_{j=1}^{p-1}\frac{\zeta_m^{P(j/\nu)}}{j}(1-\zeta_p^j) = \nu\sum_{j=1}^{p-1}\frac{\zeta_m^{P(j/\nu)}}{j}\left(\sum_{i=1}^{j}\binom{j}{i}(-1)^{i+1}(1-\zeta_p)^i\right)$$

$$= \nu\sum_{i=1}^{p-1}\left(\sum_{j=1}^{p-1}\frac{\binom{j}{i}}{j}\zeta_m^{P(j/\nu)}\right)(-1)^{i+1}(1-\zeta_p)^i \bmod p.$$

Now $\binom{j}{i} \equiv \binom{\nu P(j/\nu)}{i} \bmod p$, as $\nu P(j/\nu) \equiv j \bmod p$. It follows that

$$\sum_{j=1}^{p-1}\frac{\binom{j}{i}}{j}\zeta_m^{P(j/\nu)} \equiv \sum_{j=1}^{p-1}\frac{\frac{1}{\nu}\binom{\nu P(j/\nu)}{i}}{j/\nu}\zeta_m^{P(j/\nu)} \equiv \sum_{j=1}^{p-1}\frac{\frac{1}{\nu}\binom{\nu P(j/\nu)}{i}}{P(j/\nu)}\zeta_m^{P(j/\nu)}$$

$$= \sum_{j=1}^{p-1}\frac{\frac{1}{\nu}\binom{\nu j}{i}}{j}\zeta_m^j \bmod p.$$

We then have

$$\sum_{j=1}^{p-1}\frac{\zeta_m^j}{j}(1-\zeta_p^{\nu j}) \equiv \sum_{i=1}^{p-1}\left(\sum_{j=1}^{p-1}\frac{\binom{\nu j}{i}}{j}\zeta_m^j\right)(-1)^{i+1}(1-\zeta_p)^i \bmod p.$$

This completes the proof.

Let $g_i(X)$ $(1 \le i \le p-1)$ be a polynomial with coefficients in $\mathbb{F}_p$ such that $g_i(0) = 0$ and of degree $\le i$. We define a map $\widetilde{\tau}_\nu$ $(1 \le \nu \le p-1)$ from $\mathbb{F}_p[X]$ into itself by $\widetilde{\tau}_\nu(g(X)) = g(\nu X)$ for all $g(X) \in \mathbb{F}_p[X]$. Let $\mathbf{N}_i$ $(1 \le i \le p-1)$ be the $i \times i$ matrix

$$\mathbf{N}_i = \begin{pmatrix} 1 & 1 & \dots & 1 \\ 2^i & 2^{i-1} & \dots & 2 \\ \vdots & \vdots & \ddots & \vdots \\ i^i & i^{i-1} & \dots & i \end{pmatrix},$$

where each component represents a corresponding residue class $\bmod p$. Then it is clear that

$$\mathbf{N}_i = \begin{pmatrix} 1 & & & 0 \\ & 2 & & \\ & & \ddots & \\ 0 & & & i \end{pmatrix} \begin{pmatrix} 1 & 1 & \dots & 1 \\ 2^{i-1} & 2^{i-2} & \dots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ i^{i-1} & i^{i-2} & \dots & 1 \end{pmatrix},$$

therefore $\det \mathbf{N}_i \neq 0$, and

$$\mathbf{N}_i \begin{pmatrix} a_i X^i \\ a_{i-1} X^{i-1} \\ \vdots \\ a_1 X \end{pmatrix} = \begin{pmatrix} \widetilde{\tau}_1(g_i(X)) \\ \widetilde{\tau}_2(g_i(X)) \\ \vdots \\ \widetilde{\tau}_i(g_i(X)) \end{pmatrix},$$

where $g_i(X) = a_i X^i + a_{i-1} X^{i-1} + \ldots + a_1 X$.

Let $(c_{i,1}\ c_{i,2}\ \ldots\ c_{i,i})$ be the first row of $\mathbf{N}_i^{-1}$. Then

$$a_i X^i = c_{i,1}\widetilde{\tau}_1(g_i(X)) + c_{i,2}\widetilde{\tau}_2(g_i(X)) + \ldots + c_{i,i}\widetilde{\tau}_i(g_i(X)).$$

Letting $\widetilde{C}_i = c_{i,1}\widetilde{\tau}_1 + \ldots + c_{i,i}\widetilde{\tau}_i$, we write $a_i X^i = \widetilde{C}_i(g_i(X))$, that is

$$\widetilde{C}_i(g_i(X)) = \begin{cases} 0 & \text{if } \deg g_i(X) < i, \\ a_i X^i & \text{if } \deg g_i(X) = i. \end{cases}$$

Now we take $\binom{j}{i}$, $1 \leq i \leq p-2$, for a polynomial in an indeterminate j with coefficients in $\mathbb{F}_p$.

Since $\binom{j}{i} = (1/i!)j^i +$ (polynomial with degree $\leq i-1$), for k $(0 \leq k \leq p-3)$ we have

$$\widetilde{C}_{k+1}\binom{j}{i} = \begin{cases} 0 & \text{if } i < k+1, \\ \dfrac{1}{(k+1)!} j^{k+1} & \text{if } i = k+1, \\ * & \text{if } i > k+1, \end{cases}$$

where $*$ means some polynomial in $\mathbb{F}_p[j]$, irrelevant for our purpose.

Let τ_ν $(1 \leq \nu \leq p-1)$ be an automorphism of $\mathbb{Q}(\zeta_{mp})$ over $\mathbb{Q}$ such that $\tau_\nu : \zeta_p \mapsto \zeta_p^\nu$ and $\tau_\nu : \zeta_m \mapsto \zeta_m$, and C_i $(1 \leq i \leq p-1)$ be the element $c_{i,1}\tau_1 + c_{i,2}\tau_2 + \ldots + c_{i,i}\tau_i$ of the group ring of $\mathrm{Gal}(\mathbb{Q}(\zeta_{mp})/\mathbb{Q})$ over $\mathbb{F}_p$ (we write its action on $\mathbb{F}(K)$ additively). Then we obtain the following:

LEMMA 2.3. *For each k, $0 \leq k \leq p-3$, we have*

$$\begin{aligned} &C_{k+1}(f(\zeta_m) - f(\zeta_m\zeta_p)) \\ &\quad \equiv \frac{1}{(k+1)!}\left(\frac{1}{1-\zeta_m^p}\sum_{j=1}^{p-1} j^k \zeta_m^j\right)(-1)^k(1-\zeta_p)^{k+1} \\ &\qquad + \frac{1}{1-\zeta_m^p}\sum_{i=k+2}^{p-2}\left(\sum_{j=1}^{p-1}\frac{\widetilde{C}_{k+1}\binom{j}{i}}{j}\zeta_m^j\right)(-1)^{i+1}(1-\zeta_p)^i \bmod p. \end{aligned}$$

P r o o f. By Lemma 2.2,

$$\begin{aligned} \tau_\nu(f(\zeta_m) - f(\zeta_m\zeta_p)) &= f(\zeta_m) - f(\zeta_m\zeta_p^\nu) \\ &\equiv \frac{1}{1-\zeta_m^p}\sum_{i=1}^{p-2}\left(\sum_{j=1}^{p-1}\frac{\widetilde{\tau}_\nu\binom{j}{i}}{j}\zeta_m^j\right)(-1)^{i+1}(1-\zeta_p)^i \bmod p. \end{aligned}$$

Consequently,

$$\begin{aligned}
&C_{k+1}(f(\zeta_m)-f(\zeta_m\zeta_p))\\
&\quad\equiv \frac{1}{1-\zeta_m^p}\sum_{i=1}^{p-2}\Bigg(\sum_{j=1}^{p-1}\frac{\widetilde{C}_{k+1}\binom{j}{i}}{j}\zeta_m^j\Bigg)(-1)^{i+1}(1-\zeta_p)^i\\
&\quad\equiv \frac{1}{1-\zeta_m^p}\Bigg(\sum_{j=1}^{p-1}\frac{\widetilde{C}_{k+1}\binom{j}{k+1}}{j}\zeta_m^j\Bigg)(-1)^{k}(1-\zeta_p)^{k+1}\\
&\qquad+\frac{1}{1-\zeta_m^p}\sum_{i=k+2}^{p-2}\Bigg(\sum_{j=1}^{p-1}\frac{\widetilde{C}_{k+1}\binom{j}{i}}{j}\zeta_m^j\Bigg)(-1)^{i+1}(1-\zeta_p)^i\\
&\quad\equiv \frac{1}{1-\zeta_m^p}\Bigg(\sum_{j=1}^{p-1}\frac{1}{(k+1)!}j^k\zeta_m^j\Bigg)(-1)^{k}(1-\zeta_p)^{k+1}\\
&\qquad+\frac{1}{1-\zeta_m^p}\sum_{i=k+2}^{p-2}\Bigg(\sum_{j=1}^{p-1}\frac{\widetilde{C}_{k+1}\binom{j}{i}}{j}\zeta_m^j\Bigg)(-1)^{i+1}(1-\zeta_p)^i \bmod p,
\end{aligned}$$

as desired.

We define, for $k=0,1,\dots,p-2$ and n ($\in\mathbb{N}$) prime to p,

$$J_k(n)=\frac{1}{1-\zeta_n^p}\sum_{j=1}^{p-1}j^k\zeta_n^j \quad\text{when } n\ge 2 \qquad\text{and}\qquad J_k(1)=0.$$

We can deduce that

$$J_0(n)=\frac{1}{1-\zeta_n}-\frac{1}{1-\zeta_n^p}=(1-\sigma_p)\frac{1}{1-\zeta_n}$$

and

$$J_k(n)^{\sigma_{-1}}\equiv(-1)^{k+1}J_k(n) \bmod p$$

for $n\ge 2$ by easy calculation, where σ_{-1} denotes the automorphism which sends ζ_n to ζ_n^{-1}.

Lemma 2.4. *For each k $(1\le k\le p-2)$ we have*

$$J_k(m)\equiv\sum_{l=1}^{m-1}\Bigg(\sum_{j=1,\,M(l/p)\ge M(j/p)\ne 0}^{p-1}j^k\Bigg)\zeta_m^l \bmod p.$$

Proof. From the equality $-m/(1-\zeta_m)=\sum_{l=1}^{m-1}l\zeta_m^l$, we obtain

$$\frac{-m}{1-\zeta_m^p}=\sum_{l=1}^{m-1}l\zeta_m^{lp}$$

and

$$\frac{-m\zeta_m^j}{1-\zeta_m^p} = \sum_{l=1}^{m-1} l\zeta_m^{lp+j} = \sum_{l=1}^{m-1} l\zeta_m^{M(lp+j)}, \qquad 1 \le j \le p-1,$$

where $M(*)$ is the same as in Section 1. Now, since $M((M(lp+j)-j)/p) = l$ and

$$\{M(lp+j) : l = 1, \dots, m-1\} = \{0, 1, \dots, m-1\} \backslash \{M(j)\},$$

we obtain

$$\begin{aligned}\frac{-m\zeta_m^j}{1-\zeta_m^p} &= \sum_{l=1}^{m-1} M\left(\frac{M(lp+j)-j}{p}\right)\zeta_m^{M(lp+j)} = \sum_{l=0}^{m-1} M\left(\frac{l-j}{p}\right)\zeta_m^l \\ &= \sum_{l=1}^{m-1} M\left(\frac{l-j}{p}\right)\zeta_m^l + M\left(\frac{-j}{p}\right)(-\zeta_m - \zeta_m^2 - \dots - \zeta_m^{m-1}) \\ &= \sum_{l=1}^{m-1} \left\{M\left(\frac{l-j}{p}\right) - M\left(\frac{-j}{p}\right)\right\}\zeta_m^l.\end{aligned}$$

Therefore

$$\begin{aligned}J_k(m) &= -\frac{1}{m}\sum_{j=1}^{p-1} \frac{-m\zeta_m^j}{1-\zeta_m^p} j^k \\ &= -\frac{1}{m}\sum_{j=1}^{p-1} j^k \left\{\sum_{l=1}^{m-1}\left(M\left(\frac{l-j}{p}\right) - M\left(\frac{-j}{p}\right)\right)\zeta_m^l\right\},\end{aligned}$$

that is,

$$J_k(m) = -\frac{1}{m}\sum_{l=1}^{m-1}\left\{\sum_{j=1}^{p-1} j^k\left(M\left(\frac{l-j}{p}\right) - M\left(\frac{-j}{p}\right)\right)\right\}\zeta_m^l. \tag{2}$$

It is clear that

$$M\left(\frac{l-j}{p}\right) = \begin{cases} M(l/p) - M(j/p) & \text{if } M(l/p) \ge M(j/p), \\ M(l/p) - M(j/p) + m & \text{if } M(l/p) < M(j/p), \end{cases}$$

and

$$M\left(\frac{l-j}{p}\right) - M\left(\frac{-j}{p}\right) = \begin{cases} M(l/p) & \text{if } M(j) = 0, \\ M((l-j)/p) - \{m - M(j/p)\} & \\ \quad = M((l-j)/p) + M(j/p) - m & \text{if } M(j) \ne 0. \end{cases}$$

For these reasons,

$$M\left(\frac{l-j}{p}\right) - M\left(\frac{-j}{p}\right) = \begin{cases} M(l/p) - m & \text{if } M(l/p) \ge M(j/p) \ne 0, \\ M(l/p) & \text{if } M(l/p) < M(j/p) \text{ or } M(j) = 0. \end{cases}$$

Substituting this in (2), we have

$$\begin{aligned} J_k(m) = & -\frac{1}{m}\sum_{l=1}^{m-1}\Big\{ \sum_{j=1,\, M(l/p)\ge M(j/p)\ne 0}^{p-1} j^k(M(l/p)-m) \\ & + \sum_{j=1,\, M(l/p)<M(j/p) \text{ or } M(j)=0}^{p-1} j^k M(l/p)\Big\}\zeta_m^l \\ = & -\frac{1}{m}\sum_{l=1}^{m-1}\Big\{M(l/p)\sum_{j=1}^{p-1} j^k - m \sum_{j=1,\, M(l/p)\ge M(j/p)\ne 0}^{p-1} j^k\Big\}\zeta_m^l. \end{aligned}$$

The result follows from a well known fact that $\sum_{j=1}^{p-1} j^k \equiv 0 \bmod p$.

Lemma 2.5. *We have*

$$J_k(m) \equiv (-m)^k \sum_{l=1}^{m-1} S_k\Big(-\frac{l}{m}\Big)\zeta_m^l \bmod p, \qquad 1 \le k \le p-2.$$

Proof. It is sufficient to prove

$$\sum_{j=1,\, M(l/p)\ge M(j/p)\ne 0}^{p-1} j^k \equiv (-m)^k S_k\Big(-\frac{l}{m}\Big) \bmod p. \tag{3}$$

We deal first with the case where $m < p$. Let $x_i = P(-i/m)$ and $y_i = (i + x_i m)/p \in \mathbb{Z}$ for each i $(1 \le i \le p-1)$, where $P(*)$ is the same as in the proof of Lemma 2.2. Then we have $1 \le y_i \le m$.

Suppose that $x_i < x_j$ for $i \ne j$, $1 \le i, j \le p-1$. Then, as $j - i = (y_j - y_i)p - (x_j - x_i)m$ and $-(p-2) \le j - i$, we have

$$y_j - y_i \ge \frac{-(p-2)+m}{p} = -1 + \frac{m+2}{p} > -1.$$

Therefore, $y_j \ge y_i$ if $x_j > x_i$.

For each l $(1 \le l \le m-1)$, let

$$A_l = \{j : 1 \le j \le p-1, M(l/p) \ge M(j/p) \ne 0\}.$$

Since $y_l \ne m$, or $1 \le y_l \le m-1$, and $M(j/p) = M(y_j)$, we have

$$\begin{aligned} A_l &= \{j : 1 \le j \le p-1,\ M(y_l) \ge M(y_j) \ne 0\} \\ &= \{j : 1 \le j \le p-1,\ M(y_l) \ge M(y_j),\ y_j \ne m\} \\ &= \{j : 1 \le j \le p-1,\ y_l \ge y_j\}. \end{aligned}$$

If $m < i \le p-1$, we have $i - m = y_i p - (x_i + 1)m$; therefore $x_{i-m} = x_i + 1$ and $y_{i-m} = y_i$. For that reason, any index i, with common value y_i, can be represented in the form $i = j + m\nu$ $(1 \le j \le m, \mathbb{Z} \ni \nu \ge 0)$ and, for such i's, the maximal value of x_i equals x_j.

Consequently,

$$A_l = \{j : 1 \le j \le p-1,\ x_j \le x_l\}$$

and

$$\begin{aligned}\sum_{j=1,\, M(l/p)\ge M(j/p)\ne 0}^{p-1} j^k &= (-m)^k \sum_{j\in A_l} \Big(-\frac{j}{m}\Big)^k \equiv (-m)^k \sum_{j\in A_l} x_j^k \\ &= (-m)^k (1^k + 2^k + \ldots + x_l^k) = (-m)^k S_k(x_l) \\ &\equiv (-m)^k S_k\Big(-\frac{l}{m}\Big) \bmod p,\end{aligned}$$

as desired.

Next we consider the case where $p < m$. Let again $x_i = P(-i/m)$ and $y_i = (i + x_i m)/p \in \mathbb{Z}$ for i $(0 \le i \le m-1)$. Since $0 \le y_i p = i + x_i m \le m - 1 + (p-1)m = pm - 1$, we have $0 \le y_i \le m - 1/p$, that is, $0 \le y_i \le m-1$. It is clear that $\{x_i : 0 \le i \le p-1\} = \{0, 1, \ldots, p-1\}$. Since $i - j = (y_i - y_j)p - (x_i - x_j)m$ for $0 \le i, j \le m-1$, we see that $x_i = x_j$ if and only if $i \equiv j \bmod p$, and that $y_i < y_j$ if $x_i < x_j$. There exist i_0 and ν_i $(0 \le i_0 \le p-1,\ 1 \le \nu_i)$ such that $i = i_0 + \nu_i p$ for each i $(p \le i \le m-1)$. Since $i = y_{i_0} p - x_{i_0} m + \nu_i p = (y_{i_0} + \nu_i)p - x_{i_0} m$, we have $y_i = y_{i_0} + \nu_i$ and $x_i = x_{i_0}$.

Consequently, for l $(1 \le l \le m-1)$, we have

$$\begin{aligned}A_l &= \{j : 1 \le j \le p-1, M(l/p) \ge M(j/p)\} = \{j : 1 \le j \le p-1, y_l \ge y_j\} \\ &= \{j : 1 \le j \le p-1, y_{l_0} \ge y_j\} = \{j : 1 \le j \le p-1, x_{l_0} \ge x_j\}.\end{aligned}$$

Now, clearly, $-l/m \equiv -l_0/m \equiv x_{l_0} \bmod p$. Hence

$$\begin{aligned}\sum_{j\in A_l} j^k &= \sum_{j=1, x_j \le x_{l_0}}^{p-1} j^k \\ &= (-m)^k \sum_{j=1, x_j \le x_{l_0}}^{p-1} \Big(-\frac{j}{m}\Big)^k \equiv (-m)^k \sum_{j=1, x_j \le x_{l_0}}^{p-1} x_j^k \\ &= (-m)^k (1^k + 2^k + \ldots + x_{l_0}^k) = (-m)^k S_k(x_{l_0}) \\ &\equiv (-m)^k S_k\Big(-\frac{l}{m}\Big) \bmod p.\end{aligned}$$

We have just completed the proof of Lemma 2.5.

3. $I_k(m)$ as a partial sum of $J_k(m)$. For any divisor d of m we define

$$M_d = \Big\{l : l = \frac{m}{d}\nu,\ 1 \le \nu \le d,\ (\nu, d) = 1\Big\}.$$

It is clear that $\varphi(d) = \sharp M_d$ (the cardinality of M_d), $M_1 = \{m\}$, $\{1, 2, \ldots, m\} = \bigcup_{d|m} M_d$ (disjoint union), and $M_d = \{l : 1 \le l \le m, (l, m) = m/d\}$. Now we have, from Lemma 2.5, for $k = 1, \ldots, p-2$,

$$J_k(m) \equiv (-m)^k \sum_{l=1}^{m} S_k\Big(-\frac{l}{m}\Big)\zeta_m^l = (-m)^k \sum_{d|m} {\sum_{\nu=1}^{d}}' S_k\Big(-\frac{\frac{m}{d}\nu}{m}\Big)\zeta_m^{(m/d)\nu}$$

$$= (-m)^k \sum_{d|m} {\sum_{\nu=1}^{d}}' S_k\Big(-\frac{\nu}{d}\Big)\zeta_d^{\nu} \bmod p,$$

where $\sum_{\nu=1}^{d\prime}$ is the same as in Section 1. So, we have

$$(-m)^{-k} J_k(m) \equiv \sum_{d|m} I_k(d) \bmod p.$$

By the Möbius inversion formula, it follows that

$$I_k(m) \equiv \sum_{d|m} \{\mu(m/d)(-d)^{-k} J_k(d)\} \bmod p$$

for k $(1 \le k \le p-2)$, where μ is the Möbius function. Each $J_k(d) \bmod p$ $(d \,|\, m)$ belongs to $\overline{V}_k$ by the definition, so is $I_k(m) \bmod p$.

We have thus proved Theorem 1(1).

Lemma 3.1. *For all $k \in \mathbb{N}$, we have*

$$S_k(-X) = (-1)^{k+1} S_k(X-1).$$

Proof. From the definition of $S_k(X)$, we have $S_k(n+1) = (n+1)^k + S_k(n)$ for all $n \in \mathbb{N}$. Hence

$$S_k(X+1) = (X+1)^k + S_k(X).$$

Using this formula, we see that

$$\begin{aligned} S_k(-n) &= -(-n+1)^k + S_k(-n+1) \\ &= -(-n+1)^k - (-n+2)^k + S_k(-n+2) \\ &= \ldots = -(-n+1)^k - (-n+2)^k - \ldots - (-1)^k + S_k(-1) \\ &= (-1)^{k+1}\{1^k + 2^k + \ldots + (n-1)^k\} = (-1)^{k+1} S_k(n-1), \end{aligned}$$

for all $n \in \mathbb{N}$. This proves our lemma.

The next two lemmas, on properties of $I_k(m)$, will be used in the following section.

Lemma 3.2. *For all k $(1 \le k \le p-2)$, we have*

$$I_k(m)^{\sigma_{-1}} = (-1)^{k+1} I_k(m).$$

P r o o f.

$$\begin{aligned} I_k(m)^{\sigma_{-1}} &= \sum_{l=1}^{m}{}' S_k\Big(-\frac{l}{m}\Big)\zeta_m^{m-l} = \sum_{l=1}^{m}{}' S_k\Big(-\frac{m-l}{m}\Big)\zeta_m^{l} \\ &= \sum_{l=1}^{m}{}' S_k\Big(\frac{l}{m}-1\Big)\zeta_m^{l} = (-1)^{k+1}\sum_{l=1}^{m}{}' S_k\Big(-\frac{l}{m}\Big)\zeta_m^{l} \\ &= (-1)^{k+1} I_k(m). \end{aligned}$$

Lemma 3.3. *For $k = 0$, we have*

$$I_0(m)^{\sigma_{-1}} + I_0(m) = -\mu(m).$$

P r o o f.

$$\begin{aligned} I_0(m)^{\sigma_{-1}} &= \sum_{l=1}^{m}{}' \Big(-\frac{l}{m}\Big)\zeta_m^{-l} = \sum_{l=1}^{m}{}' \Big(-\frac{m-l}{m}\Big)\zeta_m^{l} \\ &= -\sum_{l=1}^{m}{}' \zeta_m^{l} - \sum_{l=1}^{m}{}' \Big(-\frac{l}{m}\Big)\zeta_m^{l} = -\mu(m) - I_0(m). \end{aligned}$$

This completes the proof of the lemma.

4. Determinant of $\mathbf{B}_k(m)$. Let $\mathbf{A}_k(m)$ and $\mathbf{B}_k(m)$ $(0 \le k \le p-2)$ be as in Section 1. Recall that

$$G = \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) = (\mathbb{Z}/m\mathbb{Z})^{\times} = \{\sigma_r : \zeta_m \mapsto \zeta_m^r : 1 \le r < m,\ (r,m) = 1\};$$

we shall identify G with $\{l : 1 \le l < m,\ (l,m) = 1\}$.

Let $H = \mathrm{Gal}(\mathbb{Q}(\zeta_m)^+/\mathbb{Q}) = (\mathbb{Z}/m\mathbb{Z})^{\times}/\{\pm 1\}$; we shall identify H with $\{l : 1 \le l < m/2,\ (l,m) = 1\}$. By Lemma 3.1,

$$S_k\Big(-\frac{m-l}{m}\Big) = (-1)^{k+1} S_k\Big(-\frac{l}{m}\Big), \qquad k \in \mathbb{N}. \tag{4}$$

Now, let us prove Theorem 2 and the first part of Theorem 4. First we assume k $(1 \le k \le p-2)$ is odd. Then, by means of (4), we can take $S_k(-l/m)$ for a function on H. Then it is easily verified, by a result on the group determinant, that

$$\det \mathbf{B}_k(m) = \prod_{\chi \in \widehat{H}} \sum_{l \in H} S_k\Big(-\frac{l}{m}\Big)\chi(l).$$

Moreover, by (4),

$$\sum_{l \in H} S_k\Big(-\frac{l}{m}\Big)\chi(l) = \frac{1}{2}\sum_{l \in G} S_k\Big(-\frac{l}{m}\Big)\chi(l)$$

for all $\chi \in \widehat{H}$ (the set of all even characters in $\widehat{G}$). Therefore,

$$\det \mathbf{B}_k(m) = \left(\frac{1}{2}\right)^{\varphi(m)/2} \prod_{\widehat{G} \ni \chi:\text{even}} \sum_{l \in G} S_k\left(-\frac{l}{m}\right)\chi(l). \tag{5}$$

Next we assume k is even. We fix an arbitrary odd character ξ in $\widehat{G}$. Then, from (4), we have

$$S_k\left(-\frac{m-l}{m}\right) = -S_k\left(-\frac{l}{m}\right),$$

so that $S_k(-l/m)\xi(l)$ can be regarded as a function on H. Hence, similarly to the case of k odd, we have

$$\begin{aligned}
\det\left(S_k\left(-\frac{M(l/r)}{m}\right)\xi\left(M\left(\frac{l}{r}\right)\right)\right)_{l,r\in H}
&= \prod_{\chi\in\widehat{H}} \sum_{l\in H} S_k\left(-\frac{l}{m}\right)\xi(l)\chi(l) \\
&= \prod_{\chi\in\widehat{H}} \frac{1}{2}\sum_{l\in G} S_k\left(-\frac{l}{m}\right)\xi(l)\chi(l) \\
&= \left(\frac{1}{2}\right)^{\varphi(m)/2} \prod_{\widehat{G}\ni\chi:\text{even}} \sum_{l\in G} S_k\left(-\frac{l}{m}\right)\xi(l)\chi(l) \\
&= \left(\frac{1}{2}\right)^{\varphi(m)/2} \prod_{\widehat{G}\ni\chi:\text{odd}} \sum_{l\in G} S_k\left(-\frac{l}{m}\right)\chi(l).
\end{aligned}$$

On the other hand, as $\xi(M(l/r)) = \xi(l)\xi(r^{-1})$,

$$\begin{aligned}
&\begin{pmatrix} & \vdots & \\ \dots & S_k\left(-\dfrac{M(l/r)}{m}\right)\xi\left(M\left(\dfrac{l}{r}\right)\right) & \dots \\ & \vdots & \end{pmatrix}_{r,l\in H} \\
&= \begin{pmatrix} \ddots & & 0 \\ & \xi(r^{-1}) & \\ 0 & & \ddots \end{pmatrix}_{r\in H} \begin{pmatrix} & \vdots & \\ \dots & S_k\left(-\dfrac{M(l/r)}{m}\right) & \dots \\ & \vdots & \end{pmatrix}_{r,l\in H} \begin{pmatrix} \ddots & & 0 \\ & \xi(l) & \\ 0 & & \ddots \end{pmatrix}_{l\in H}.
\end{aligned}$$

Consequently,

$$\det \mathbf{B}_k(m) = \left(\frac{1}{2}\right)^{\varphi(m)/2} \prod_{\widehat{G}\ni\chi:\text{odd}} \sum_{l\in G} S_k\Big(-\frac{l}{m}\Big)\chi(l). \tag{6}$$

We recall the Bernoulli numbers and polynomials defined by

$$\frac{t}{e^t-1} = \sum_{n=0}^{\infty} B_n t^n/n! \quad \text{and} \quad B_n(X) = \sum_{i=0}^{n} \binom{n}{i} B_i X^{n-i},$$

respectively. It is well known that

$$S_k(X-1) = \frac{1}{k+1}(B_{k+1}(X) - B_{k+1}) \quad \text{for any } k \in \mathbb{N}.$$

Since

$$S_k\Big(-\frac{l}{m}\Big) = (-1)^{k+1} S_k\Big(\frac{l}{m}-1\Big) = \frac{(-1)^{k+1}}{k+1}\Big\{B_{k+1}\Big(\frac{l}{m}\Big) - B_{k+1}\Big\},$$

we have

$$\sum_{l\in G} S_k\Big(-\frac{l}{m}\Big)\chi(l) = \frac{(-1)^{k+1}}{k+1}\sum_{l=1}^{m} B_{k+1}\Big(\frac{l}{m}\Big)\chi(l) - \frac{(-1)^{k+1}}{k+1} B_{k+1}\sum_{l=1}^{m}\chi(l),$$

for any $\chi \in \widehat{G}$, where χ is understood to be a Dirichlet character defined modulo m. Clearly, $B_{k+1}\sum_{l=1}^{m}\chi(l) \neq 0$ if and only if k is odd and χ is the principal character $1_m \in \widehat{G}$, where $1_m(l) = 1$ if $(l,m) = 1$, and $1_m(l) = 0$ if $(l,m) > 1$. Moreover, in that case, $B_{k+1}\sum_{l=1}^{m}\chi(l) = B_{k+1}\varphi(m)$.

We also recall the generalized Bernoulli numbers defined by

$$B_{n,\chi} = m^{n-1}\sum_{a=1}^{m}\chi(a)B_n\Big(\frac{a}{m}\Big), \quad n \in \mathbb{N},\ \chi \in \widehat{G},$$

satisfying

$$L(1-n,\chi) = -\frac{B_{n,\chi}}{n},$$

where $L(s,\chi)$ denotes the L-function attached to χ. By elementary results on L-functions, we have, for k $(1 \le k \le p-2)$,

$$L(-k,\chi) = L(-k,\chi_1)\prod_{q|m}(1-\chi_1(q)q^k),$$

where $\prod_{q|m}$ and χ_1 are as in Section 1. It follows that

$$\sum_{l=1}^{m} B_{k+1}\Big(\frac{l}{m}\Big)\chi(l) = \frac{1}{m^k}B_{k+1,\chi} = -\frac{k+1}{m^k}L(-k,\chi)$$
$$= -\frac{k+1}{m^k}L(-k,\chi_1)\prod_{q|m}(1-\chi_1(q)q^k)$$
$$= B_{k+1,\chi_1} \times \frac{1}{m^k}\prod_{q|m}(1-\chi_1(q)q^k).$$

Now we assume that k $(1 \le k \le p-2)$ is odd. Then we have, using assertions stated above,

$$\det \mathbf{B}_k(m)$$
$$= \Big(\frac{1}{2}\Big)^{\varphi(m)/2} \prod_{\widehat{G}\ni\chi:\text{even}} \sum_{l=1}^{m} S_k\Big(-\frac{l}{m}\Big)\chi(l)$$
$$= \Big(\frac{1}{2}\Big)^{\varphi(m)/2} \prod_{\widehat{G}\ni\chi:\text{even}} \Big\{\frac{(-1)^{k+1}}{k+1}\sum_{l=1}^{m} B_{k+1}\Big(\frac{l}{m}\Big)\chi(l) - \frac{(-1)^{k+1}}{k+1}B_{k+1}\sum_{l=1}^{m}\chi(l)\Big\}$$
$$= \Big(\frac{1}{2}\Big)^{\varphi(m)/2} \prod_{\widehat{G}\ni\chi\neq 1_m:\text{even}} \Big\{\frac{(-1)^{k+1}}{k+1}(-1)\frac{k+1}{m^k}L(-k,\chi_1)\prod_{q|m}(1-\chi_1(q)q^k)\Big\}$$
$$\times \Big\{\frac{(-1)^{k+1}}{k+1}\sum_{l=1}^{m} B_{k+1}\Big(\frac{l}{m}\Big)1_m(l) - \frac{(-1)^{k+1}}{k+1}B_{k+1}\varphi(m)\Big\}$$
$$= \Big(\frac{1}{2}\Big)^{\varphi(m)/2} \prod_{\widehat{G}\ni\chi\neq 1_m:\text{even}} \Big\{\frac{-1}{m^k}L(-k,\chi_1)\prod_{q|m}(1-\chi_1(q)q^k)\Big\}$$
$$\times \Big\{\frac{-1}{k+1}\cdot\frac{k+1}{m^k}L(-k,\chi^0)\prod_{q|m}(1-q^k) - (-1)^k L(-k,\chi^0)\varphi(m)\Big\}$$
$$= \Big(\frac{1}{2}\Big)^{\varphi(m)/2}\Big(\frac{-1}{m^k}\Big)^{\varphi(m)/2} \prod_{\widehat{G}\ni\chi:\text{even}} L(-k,\chi_1)$$
$$\times \prod_{\widehat{G}\ni\chi\neq 1_m:\text{even}} \prod_{q|m}(1-\chi_1(q)q^k)\Big\{\prod_{q|m}(1-q^k) - m^k\varphi(m)\Big\},$$

where χ^0 denotes the primitive character with conductor 1.

Using the expression

$$\zeta_{\mathbb{Q}(\zeta_m)^+}(-k) = \prod_{\widehat{G}\ni\chi:\text{even}} L(-k,\chi_1),$$

we can obtain the case of k odd in Theorem 2 and the first part of Theorem 4.

Next we assume that k $(1 \le k \le p-2)$ is even. Then

$$\begin{aligned}
\det \mathbf{B}_k(m) &= \left(\frac{1}{2}\right)^{\varphi(m)/2} \prod_{\widehat{G}\ni\chi:\text{odd}} \sum_{l=1}^{m} S_k\Big(-\frac{l}{m}\Big)\chi(l) \\
&= \left(\frac{1}{2}\right)^{\varphi(m)/2} \prod_{\widehat{G}\ni\chi:\text{odd}} \left\{\frac{(-1)^{k+1}}{k+1}\sum_{l=1}^{m} B_{k+1}\left(\frac{l}{m}\right)\chi(l)\right\} \\
&= \left(\frac{1}{2}\right)^{\varphi(m)/2} \prod_{\widehat{G}\ni\chi:\text{odd}} \left\{\frac{-1}{k+1}(-1)\frac{k+1}{m^k}L(-k,\chi_1)\right. \\
&\qquad\qquad \left. \times \prod_{q\mid m}(1-\chi_1(q)q^k)\right\} \\
&= \left(\frac{1}{2m^k}\right)^{\varphi(m)/2} \prod_{\widehat{G}\ni\chi:\text{odd}} L(-k,\chi_1) \prod_{\widehat{G}\ni\chi:\text{odd}} \prod_{q\mid m}(1-\chi_1(q)q^k).
\end{aligned}$$

Therefore the expression

$$\frac{\zeta_{\mathbb{Q}(\zeta_m)}}{\zeta_{\mathbb{Q}(\zeta_m)^+}}(-k) = \prod_{\widehat{G}\ni\chi:\text{odd}} L(-k,\chi_1)$$

concludes the proof of the case of k even in Theorem 2.

5. On $I_0(m)$ mod p. Let M_d, $d \mid m$, be the same as in Section 3. Then

$$\sum_{j=1}^{m} \frac{j}{m}\zeta_m^j = \sum_{d\mid m}\sum_{\nu=1}^{d}{}' \frac{(m/d)\nu}{m}\zeta_m^{(m/d)\nu} = \sum_{d\mid m}\sum_{\nu=1}^{d}{}' \frac{\nu}{d}\zeta_d^{\nu}.$$

Hence, by the Möbius inversion formula,

$$\sum_{j=1}^{m}{}' \frac{j}{m}\zeta_m^j = \sum_{d\mid m}\mu\left(\frac{m}{d}\right)\sum_{\nu=1}^{d}\frac{\nu}{d}\zeta_d^{\nu}.$$

Since

$$\sum_{\nu=1}^{d-1}\frac{\nu}{d}\zeta_d^{\nu} = \frac{-1}{1-\zeta_d} \qquad \text{for all } d>1,$$

it follows that

$$\begin{aligned}\sum_{j=1}^{m}{}' \frac{j}{m}\zeta_m^j &= \sum_{1\neq d|m} \mu\left(\frac{m}{d}\right)\left(\frac{-1}{1-\zeta_d}+1\right)+\mu(m)\\ &= -\sum_{1\neq d|m} \mu\left(\frac{m}{d}\right)\frac{1}{1-\zeta_d}+\sum_{d|m}\mu\left(\frac{m}{d}\right)\\ &= -\sum_{1\neq d|m} \mu\left(\frac{m}{d}\right)\frac{1}{1-\zeta_d}.\end{aligned}$$

From definitions of $J_k(n)$ and $I_k(m)$, we obtain

$$(1-\sigma_p)I_0(m)=\sum_{d|m}\mu\left(\frac{m}{d}\right)J_0(d). \tag{7}$$

This proves Theorem 1(2).

Recall that

$$\mathbf{A}_0(m)=-\frac{1}{m}\left(M\left(\frac{l}{r}\right)\right)_{r,l\in G},\qquad \mathbf{B}_0(m)=-\frac{1}{m}\left(M\left(\frac{l}{r}\right)\right)_{r,l\in H}.$$

The theorem of Tateyama [5] tells us that

$$\det\left(M\left(\frac{l}{r}\right)\right)_{r,l\in H} = \begin{cases}(-m)^{\varphi(m)/2-1}2^{g(m)-1}h^-(\mathbb{Q}(\zeta_m)) & \text{if } g(m)=g^+(m),\\ 0 & \text{if } g(m)\neq g^+(m).\end{cases}$$

Let $h=\frac{1}{2}\varphi(m)$ and let r_i $(1\le i\le 2h)$ be natural numbers such that $r_i<r_j$ if $i<j$ and $\{l: 1\le l<m,\ (l,m)=1\}=\{r_1,r_2,\dots,r_{2h}\}$. We shall index the rows and the columns of $\mathbf{A}_0(m)$ and $\mathbf{B}_0(m)$ by $i=1,\dots,2h$ and $i=1,\dots,h$, respectively.

Lemma 5.1. *Assume that $g(m)=g^+(m)$ and that p does not divide $h^-(\mathbb{Q}(\zeta_m))$. Then*

$$\{I_0(m)^{\sigma_r} \bmod p : r=r_1,\dots,r_{h+1}\}$$

is a linearly independent system in $\mathbb{Z}[\zeta_m]/(p)$ over $\mathbb{F}_p$.

Proof. It is easy to see that $r_h=(m-1)/2$, $M(r_h^{-1})=m-2$, $r_{h+1}=(m+1)/2$, and $M(r_{h+1}^{-1})=2$. Therefore the $(h+1)$th row in $(M(r_j/r_i))_{1\le i,j\le 2h}$ is

$$(2r_1\ 2r_2\ \dots\ 2r_h\ M(2r_{h+1})\ M(2r_{h+2})\ *\ \dots\ *).$$

Add $(-2)\times$(the first row) to the $(h+1)$th row in $(M(r_j/r_i))_{1\le i,j\le 2h}$. Then the $(h+1)$th row becomes

$$(0\ \dots\ 0\ 1-2r_{h+1}\ *\ \dots\ *)=(0\ \dots\ 0\ -m\ *\ \dots\ *).$$

Consequently, by our assumptions,

$$\begin{aligned}\det(M(r_j/r_i))_{1\le i,j\le h+1} &= (-m)\times\det(M(r_j/r_i))_{1\le i,j\le h}\\ &= (-m)^{\varphi(m)/2}2^{g(m)-1}h^-(\mathbb{Q}(\zeta_m))\not\equiv 0 \bmod p.\end{aligned}$$

This proves our assertion.

Let W_m be the subspace of $\mathbb{Z}[\zeta_m]/(p)$ generated by

$$\{I_0(m)^{\sigma_r} \bmod p : r = r_1, r_2, \dots, r_{h+1}\}.$$

LEMMA 5.2. *W_m is a G-subspace.*

Proof. Take any $I_0(m)^{\sigma_r}$ $(r = r_1, \dots, r_{h+1})$ and $\sigma_s \in G$. If $M(sr) \le m/2$, then we have $M(sr) \in \{r_1, \dots, r_h\}$ and thus

$$\{I_0(m)^{\sigma_r}\}^{\sigma_s} \bmod p = I_0(m)^{\sigma_{M(rs)}} \bmod p \in W_m.$$

Next suppose $m/2 < M(sr)$. Then $M(-sr) = m - M(sr) \le m/2$. Since $r_{h+1} = m - r_h$ and $\sigma_{r_{h+1}} = \sigma_{-1}\sigma_{r_h}$, we have, by Lemma 3.3,

$$\begin{aligned}\{I_0(m)^{\sigma_r}\}^{\sigma_s} &= I_0(m)^{\sigma_{M(rs)}} = \{I_0(m)^{\sigma_{-1}}\}^{\sigma_{M(-sr)}}\\ &= \{-I_0(m)-\mu(m)\}^{\sigma_{M(-sr)}}\\ &= -I_0(m)^{\sigma_{M(-sr)}} - \mu(m)\\ &= -I_0(m)^{\sigma_{M(-sr)}} + I_0(m)^{\sigma_{r_h}} + I_0(m)^{\sigma_{r_{h+1}}}.\end{aligned}$$

Therefore, $\{I_0(m)^{\sigma_r}\}^{\sigma_s} \bmod p \in W_m$, and the proof is complete.

From the equation

$$I_0(m)^{\sigma_{r_{h+1}}} = -\{I_0(m)^{\sigma_{r_h}} + \mu(m)/2\} - \mu(m)/2,$$

we can take

$$\{1 \bmod p, I_0(m)^{\sigma_r} + \mu(m)/2 \bmod p : r = r_1, \dots, r_h\}$$

for another set of generators of W_m.

Let $\varepsilon_+ = (1+\sigma_{-1})/2$ and $\varepsilon_- = (1-\sigma_{-1})/2$; these are orthogonal idempotents in $\mathbb{F}_p[G]$. Let W'_m be the subspace of W_m generated by $\{1 \bmod p\}$ and W''_m the subspace of W_m generated by $\{I_0(m)^{\sigma_r} + \mu(m)/2 \bmod p : r = r_1, \dots, r_h\}$. It is easy to see that $\varepsilon_+(1 \bmod p) = 1 \bmod p$, $\varepsilon_-(1 \bmod p) = 0$, $\varepsilon_+(I_0(m)^{\sigma_r} + \mu(m)/2 \bmod p) = 0$, and $\varepsilon_-(I_0(m)^{\sigma_r} + \mu(m)/2 \bmod p) = I_0(m)^{\sigma_r} + \mu(m)/2 \bmod p$. Therefore,

$$W_m = W'_m \oplus W''_m, \quad W'_m = \varepsilon_+ W_m, \quad \text{and} \quad W''_m = \varepsilon_- W_m.$$

Note that $\dim_{\mathbb{F}_p} W'_m = 1$.

Now, we prove Theorem 3. The mapping $1-\sigma_p$ is linear from $\mathbb{Z}[\zeta_m]/(p)$ into itself. Let $\alpha \bmod p$ be any element of $\mathrm{Ker}(1-\sigma_p)$. Then, since $\alpha^{\sigma_p} \equiv \alpha \bmod p$, we have $\alpha^{\sigma_p} \equiv \alpha \bmod \wp_i$ $(i = 1, \dots, g)$, where $\wp_1, \dots, \wp_g$ are the primes of $\mathbb{Q}(\zeta_m)$ which divide p. We know σ_p is the Frobenius automorphism for p. Hence, there exist $a_i \in \mathbb{Z}$ $(i = 1, \dots, g)$ such that $\alpha \equiv a_i \bmod \wp_i$ $(i =$

$1, \ldots, g$). Consequently, $\dim_{\mathbb{F}_p} \mathrm{Ker}(1-\sigma_p) \leq g$. On the other hand, let Z and O_Z be the decomposition field of p and its ring of integers, respectively. Then it is clear that $\mathrm{Ker}(1-\sigma_p) \supset O_Z/(p)$. Since $\dim_{\mathbb{F}_p} O_Z/(p) = [Z : \mathbb{Q}] = g$, we have

$$\mathrm{Ker}(1-\sigma_p) = O_Z/(p).$$

Suppose first that p does not decompose in $\mathbb{Q}(\zeta_m)/\mathbb{Q}(\zeta_m)^+$. Then since $-1 \bmod m$ belongs to the subgroup of $(\mathbb{Z}/m\mathbb{Z})^\times$ generated by $p \bmod m$, $\beta^{\sigma_{-1}} = \beta$ for all $\beta \in O_Z$. Therefore,

$$\varepsilon_+(O_Z/(p)) = O_Z/(p), \quad \varepsilon_-(O_Z/(p)) = 0,$$

and

$$\mathrm{Ker}(1-\sigma_p) = \varepsilon_+(O_Z/(p)).$$

It follows that $W_m \cap \mathrm{Ker}(1-\sigma_p) = W'_m \cap \varepsilon_+(O_Z/(p))$, and so

$$\dim_{\mathbb{F}_p}(W_m \cap \mathrm{Ker}(1-\sigma_p)) = 1.$$

Hence, by Lemma 5.1,

$$\begin{aligned}\dim_{\mathbb{F}_p}(1-\sigma_p)W_m &= \dim_{\mathbb{F}_p} W_m - \dim_{\mathbb{F}_p}(W_m \cap \mathrm{Ker}(1-\sigma_p)) \\ &= \tfrac{1}{2}\varphi(m) + 1 - 1 = \tfrac{1}{2}\varphi(m).\end{aligned}$$

Recalling that $J_0(m)^{\sigma_{-1}} \equiv -J_0(m) \bmod p$ (from Section 2), we see that $\dim_{\mathbb{F}_p} \overline{V}_0 \leq \frac{1}{2}\varphi(m)$. Since (7) means that $(1-\sigma_p)W_m \subset \overline{V}_0$, we have $\dim_{\mathbb{F}_p} \overline{V}_0 = \frac{1}{2}\varphi(m)$ as desired.

Next suppose that p decomposes in $\mathbb{Q}(\zeta_m)/\mathbb{Q}(\zeta_m)^+$. Let $Z^+ = \mathbb{Q}(\zeta_m)^+ \cap Z$. Then, by our assumption, Z is a quadratic extension over Z^+. We have $\varepsilon_+(O_Z/(p)) = O_{Z^+}/(p)$, because $O_{Z^+}/(p) = \varepsilon_+(O_{Z^+}/(p)) \subset \varepsilon_+(O_Z/(p)) \subset O_{Z^+}/(p)$, and $\dim_{\mathbb{F}_p} \varepsilon_+(O_Z/(p)) = \dim_{\mathbb{F}_p} \varepsilon_-(O_Z/(p)) = g/2$, because $[Z^+ : \mathbb{Q}] = g/2$. From this and the decomposition

$$W_m = W'_m \oplus W''_m \qquad (\dim_{\mathbb{F}_p} W'_m = 1),$$

we obtain $\dim_{\mathbb{F}_p}(W_m \cap \mathrm{Ker}(1-\sigma_p)) \leq g/2 + 1$.

We have thus proved, using Lemma 5.1, that

$$\begin{aligned}\dim_{\mathbb{F}_p} \overline{V}_0 &\geq \dim_{\mathbb{F}_p}(1-\sigma_p)W_m = \dim_{\mathbb{F}_p} W_m - \dim_{\mathbb{F}_p}(W_m \cap \mathrm{Ker}(1-\sigma_p)) \\ &\geq \frac{1}{2}\varphi(m) + 1 - \left(\frac{g}{2} + 1\right) = \frac{1}{2}\varphi(m) - \frac{g}{2}.\end{aligned}$$

The proof of Theorem 3 is complete.

6. Fermat quotient of units of type II. It is clear that the $(p^f - 1)$th power of any unit of type II is congruent to 1 modulo p, where f is the same as in Section 1. Letting $X = \zeta_m^p$ and $\nu = f$ in Lemma 2.1, we have

$$(1-\zeta_m^p)^{p^f} \equiv 1 - \zeta_m^p - p\left(\zeta_m + \frac{\zeta_m^2}{2} + \ldots + \frac{\zeta_m^{p-1}}{p-1}\right) \bmod p^2,$$

and then

$$(1-\zeta_m^p)^{p^f-1} \equiv 1 - pf(\zeta_m) \bmod p^2. \tag{8}$$

Therefore, $f(\zeta_m) \bmod p$ is the Fermat quotient of $(1-\zeta_m^p)^{1-p^f}$ if m is composite, and

$$f(\zeta_m) = \frac{1}{1-\zeta_m^p}\sum_{j=1}^{p-1} j^{-1}\zeta_m^j \equiv \frac{1}{1-\zeta_m^p}\sum_{j=1}^{p-1} j^{p-2}\zeta_m^j = J_{p-2}(m) \bmod p.$$

From the fact proved in Section 3, we have

$$I_{p-2}(m) \equiv \sum_{d\mid m}\left\{\mu\left(\frac{m}{d}\right)(-d)J_{p-2}(d)\right\} \bmod p. \tag{9}$$

We remark that $J_{p-2}(d) \equiv f(\zeta_d) \bmod p$ is the Fermat quotient of some unit if d is composite, and is not if d is prime, because $1-\zeta_d^p$ is not a unit.

Now let $d = q$ (a prime number dividing m). Then

$$\left(\frac{1-\zeta_q^{p\nu}}{1-\zeta_q^p}\right)^{p^f-1} \qquad (2 \le \nu \le q-1)$$

is a unit with the Fermat quotient $f(\zeta_q) - f(\zeta_q^\nu) \bmod p$. Therefore, in this case, $(1-\sigma_\nu)J_{p-2}(q) \bmod p$ is the Fermat quotient of some unit.

For each ν $(2 \le \nu < m,\ (\nu, m) = 1)$, since $(\nu, q) = 1$ for any prime $q \mid m$, it follows that $(1-\sigma_\nu)J_{p-2}(q) \bmod p$ is a Fermat quotient for such q. Consequently, by (9), we see that $(1-\sigma_\nu)I_{p-2}(m) \bmod p$ is a Fermat quotient for each ν $(2 \le \nu < m,\ (\nu, m) = 1)$. This proves Theorem 1(3).

Now we shall prove the second part of Theorem 4. Note that $(1-\sigma_\nu)I_{p-2}(m) \bmod p$ belongs to $\overline{V}_{-1}$ for each ν $(2 \le \nu < m,\ (\nu, m) = 1)$. If $\det \mathbf{B}_{p-2}(m) \not\equiv 0 \bmod p$, then it follows, by the definition, that

$$\{\sigma_\nu I_{p-2}(m) \bmod p : 1 \le \nu \le m/2, (\nu, m) = 1\}$$

is a linearly independent system over $\mathbb{F}_p$, and further, so is

$$\{(1-\sigma_\nu)I_{p-2}(m) \bmod p : 2 \le \nu \le m/2, (\nu, m) = 1\}.$$

This proves $\dim_{\mathbb{F}_p} \overline{V}_{-1} \ge \frac{1}{2}\varphi(m) - 1$.

7. Fermat quotient of units of type III. Units of type III belong to $\mathbb{Q}(\zeta_p)$. From Washington [6], we easily see that, for each even i $(2 \le i \le p-3)$ and sufficiently large $N \in \mathbb{N}$, there exists a unit $E_i^{(N)}$ satisfying

$$E_i^{(N)} \equiv a_i + b_i(1-\zeta_p)^{i+(p-1)v_p(L_p(1,\omega^i))} \bmod (1-\zeta_p)^{i+2+(p-1)v_p(L_p(1,\omega^i))},$$

where $a_i, b_i \in \mathbb{Z}$ with $a_i b_i \not\equiv 0 \bmod p$, v_p is the p-adic valuation normalized by $v_p(p) = 1$, ω is the Teichmüller character, and $L_p(s, \omega^i)$ is the p-adic L-function attached to ω^i.

The proof of Theorem 1(4) is the following. Note that our assumption $B_{k+1} \not\equiv 0 \bmod p$ is equivalent to $v_p(L_p(1, \omega^{k+1})) = 0$. Then, from above,

$$\begin{aligned}\{E_{k+1}^{(N)}\}^{p-1} &\equiv a_{k+1}^{p-1} - a_{k+1}^{p-2} b_{k+1} (1-\zeta_p)^{k+1} \\ &\equiv 1 - a_{k+1}^{p-2} b_{k+1} (1-\zeta_p)^{k+1} \bmod (1-\zeta_p)^{k+3}.\end{aligned}$$

So there exists an integer $z_{k+1} \in \mathbb{Z}[\zeta_p]$ such that

$$\{E_{k+1}^{(N)}\}^{p-1} = 1 + \{-a_{k+1}^{p-2} b_{k+1} + z_{k+1}(1-\zeta_p)^2\}(1-\zeta_p)^{k+1}.$$

Moreover, there is an integer $z'_{k+1} \in \mathbb{Z}[\zeta_p]$ such that

$$\{E_{k+1}^{(N)}\}^{p(p-1)} \equiv 1 + p\{-a_{k+1}^{p-2} b_{k+1} (1-\zeta_p)^{k+1} + z'_{k+1}(1-\zeta_p)^{k+3}\} \bmod p^2.$$

Let u_k be the $(-a_{k+1}/b_{k+1})$th power of $\{E_k^{(N)}\}^{p(p-1)}$. Then

$$u_k \equiv 1 + p\{(1-\zeta_p)^{k+1} + z''_{k+1}(1-\zeta_p)^{k+3}\} \bmod p^2,$$

with some $z''_{k+1} \in \mathbb{Z}[\zeta_p]$, thus $\pi_k(\psi(u_k)) = 1 \bmod p$. The proof is complete.

References

[1] L. Carlitz, *A generalization of Maillet's determinant and a bound for the first factor of the class number*, Proc. Amer. Math. Soc. 12 (1961), 256–261.

[2] H. W. Leopoldt, *Über Fermatquotienten von Kreiseinheiten und Klassenzahlformeln modulo p*, Rend. Circ. Mat. Palermo (2) 9 (1960), 39–50.

[3] C. Levesque, *$\mathbb{Z}_p$-independent systems of units*, Proc. Japan Acad. Ser. A 68 (1992), 239–241.

[4] J. W. Sands, *Kummer's and Iwasawa's version of Leopoldt's conjecture*, Canad. Math. Bull. 31 (1988), 338–346.

[5] K. Tateyama, *Maillet's determinant*, Sci. Papers College Gen. Edu. Univ. Tokyo 32 (1982), 97–100.

[6] L. C. Washington, *Introduction to Cyclotomic Fields*, Springer, New York, 1982.

Kanagawa Prefectural Shôyô High School
7713 Izumicho, Izumi-ku
Yokohama, 245 Japan
E-mail: shimada@math.metro-u.ac.jp

Received on 31.1.1995 (2737)